INFORMATION RIGHTS REPORT

QUARTER 2 – 2015/16

1. Key Developments

Some key developments expected in the next quarter are:

- Continuing fall-out from the CJEU decision on the validity of the EU/US Safe Harbor agreement. Possible unveiling of a new version of the Safe Harbor.

- Submission of evidence to the Independent Commission on Freedom of Information. Publication of the Commission's report.

- Possible conclusion of trilogue discussions on the proposed EU Data Protection Regulation and Law Enforcement Directive.

- Award of contract for marketing strategy and logo design for privacy seals project. Launch of call for applications from prospective third party scheme providers.

- Publication of Investigatory Powers Bill. ICO's initial response and likely requirement to give evidence.

- Contributing to the review of "consent" and "opt-out" in the health sector.

- International Conference of Data Protection and Privacy Commissioners with launch of "Building Bridges" report and opportunity to participate in Global Cross Border Enforcement Cooperation Arrangement.

- Release of self-assessment toolkit aimed at SMEs.

- First monetary penalties for PECR breaches based on the new, less stringent criteria coming through.

2. Cross Sectoral Work

2.1 Data Protection

2.1.1 Proposed EU Data Protection Regulation and Law Enforcement Directive

Trilogue discussions have continued on the General Data Protection Regulation (GDPR) and some agreement has been reached. However a significant number of key issues between the Council and Parliament remain to be resolved, such as – whether explicit consent should be the single standard throughout the text, the threshold for data controllers to appoint a data protection officer, the triggers for mandatory breach notification and whether incompatible processing can be lawful if a legitimate interest condition is met. The recent Schrems judgment from the CJEU on safe harbor and international transfers (see below) will be likely to influence discussions about the chapter on international transfers and what role data protection authorities should play when law enforcement agencies from outside the EU request access to personal data from EU data controllers or data that has been transferred from the EU.

It appears unlikely that final agreement can be reached by Christmas, though this is still the official line of the institutions. Completion by the middle of 2016 seems the likely prospect, which would mean that the Regulation would come into force by the middle of 2018.

An ICO cross office group has started preparation on some aspects of implementation, working on the basis that although the detail of the text has not been agreed we can be sure about the key building blocks. The initial work of the group has focused on three of the most challenging areas of the text: mandatory breach notification, prior authorisation of data protection impact assessments and engagement with cross –EU cases via the "one stop shop" mechanism. The group is seeking to model the likely scenarios in terms of volume and how these can be mapped into existing ICO processes and structure. The group has commissioned some external research to assess the likely number of data breaches that will be reported to the ICO.

A formal ICO project board to oversee the implementation work is planned and will be convened for the first time later in 2015. This will then sit for the duration of the implementation period.

On 9 October the Council of the EU also agreed their text for the Data Protection Directive for the police and criminal justice sector. This now enables the Directive to join the GDPR in the trilogue process, as the two had always been regarded as a package by the European Commission. The Directive will have less impact in the UK and is likely to apply only to cross border law enforcement processing, due to the UK opt-out for criminal justice.

2.1.2 Code of Practice on Privacy Notices

We have held a series of workshops on the revision of the ICO Privacy Notices Code of Practice – one with the Society for Computer and Law and another with Internet Advertising Bureau. The workshops have explored the key principles contained in the code, assessing where they still work well and where the code needs to be supplemented to take account of digital services and applications. The new Code will be issued for consultation in November and will include advice on how to deliver effective privacy information for mobile devices and for connected devices in the "internet of things". The Code will focus on how privacy information should be embedded into services - using concepts like just-in-time notices and real time information, rather than just a single notice at one point in the process. We will also consult on the idea of providing a "privacy notice generator" tool on the ICO website.

2.1.3 Privacy Seals update

The tendering process for the marketing strategy and logo design has been completed and a contract will be awarded shortly. The work will include research with consumers and stakeholders. This work will be completed by early 2016.

The call for applications from third party scheme providers will be launched later in 2015, with a view to endorsing the first schemes in the first half of 2016, and then starting the accreditation process with UKAS. Depending on the scheme operators' previous background with accreditation standards it may be possible for the first schemes to be formally launched before the end of 2016.

2.1.4 Windows 10

Microsoft launched the latest version of their windows operating system in July and there has been public debate about how the system combines data, transparency of this processing to users and default settings. [redacted] The ICO has also been assessing the system in its IT lab.

2.1.5 App sweep

The Technology Team have completed their "deeper dive" into the 20 leading mobile apps, looking at privacy settings and security. This is complementary to the broader sweep that the ICO conducted with international DPAs, as part of GPEN, last year. The findings will be published in a blog during October. It will highlight a number of areas where security practice needs to be improved. The Enforcement team have also contacted the relevant app providers. The App sweep will now be extended to look apps linked to health services, including apps connected to devices such as fitness trackers.

2.1.6 Wi-fi

The ICO's proposed paper on wi-fi analytics and location has been approved by the Berlin Group of data protection authorities and will also be published as ICO guidance. The guidance explains how wi-fi location data can be used to identify individuals and how personal data may be processed. It stresses the need for clear and transparent information, and how to avoid excessive data collection.

The ICO's technology team published the results of some fieldwork testing of public wi-fi hotspots – to assess what information is collected from users and how the information is used, particularly for marketing purposes. In September a blog was published setting out in the results, highlighting a wide variation in the standard of privacy information presented to users and explanation of how the personal data may be used. We have also written to all the data controllers who operated the hotspots.

2.1.7 Parliamentary Committee Inquiries

The ICO has submitted a response to the Science and Technology Inquiry into big data and the Commissioner will give evidence in person later in October. The ICO has also submitted evidence to the House of Lords EU Subcommittee Inquiry into the European Digital Single Market Strategy. The ICO will also give evidence in person to the Committee in October, focused on the topic of online platforms.

2.1.8 Establishment of data controllers in the EU

The issue of establishment, and when the data protection authorities have jurisdiction, continues to prove challenging. As well as the Google Spain judgment from 2014 a recent judgment from the Court of Justice of the EU, Welltimo, has clarified the tests that should be applied when considering the concept of establishment under Article 4 of the Data Protection Directive. The Court has been clear that even a relatively minimal presence in an EU country will be enough – for example in Welltimo the Court considered the use of debt recovery services by an online property company establishes a connection with the data processing. The Article 29 Working Party is currently revising its opinion on applicable law and this will reflect the new CJEU judgment. It is clear that the accepted position of how certain multinational companies are established in the EU can now be challenged, particularly if they are online platforms. It is likely to lead to an examination of EU offices of multinational companies, that are not the company's main establishment, and whether those offices have sufficient connection with the processing of personal data for the data protection authority where the office is located to have jurisdiction.

2.1.9 Intervention in CJEU Cases

As will be apparent from the report and elsewhere cases in the Court of Justice of the European Union (CJEU) are having an increasing impact on the data protection work of the ICO. When cases are before the Court member states have the opportunity to intervene giving their point of view. The UK Government regularly uses this opportunity but has not been inclined to consult or even inform the ICO when doing so. We are now finalising a protocol with DCMS colleagues to ensure that we keep each other informed of relevant cases without compromising our respective roles.

2.2 Freedom of Information

Independent Commission on Freedom of Information

On 9 October the Commission launched its call for evidence, having previously announced its terms of reference on 17 July. There has been significant public debate about the composition of the taskforce. The Commission is chaired by Lord Burns; its other members are the Rt Hon Jack Straw, the Rt Hon Lord Howard of Lympne, Lord Carlile of Berriew and Dame Patricia Hodgson.

The terms of reference are:

> "The Commission will review the Freedom of Information Act 2000 ('the Act') to consider whether there is an appropriate public interest balance between transparency, accountability and the need for sensitive information to have robust protection, and whether the operation of the Act adequately recognises the need for a "safe space" for policy development and implementation and frank advice. The Commission may also consider the balance between the need to maintain public access to information, and the burden of the Act on public authorities, and whether change is needed to moderate that while maintaining public access to information."

In its call for evidence the Commission have asked the following six questions, which are somewhat broader than expected, particularly the reference to the enforcement and appeal system.

Question 1: What protection should there be for information relating to the internal deliberations of public bodies? For how long after a decision does such information remain sensitive? Should different protections apply to different kinds of information that are currently protected by sections 35 and 36?

Question 2: What protection should there be for information which relates to the process of collective Cabinet discussion and agreement? Is this information entitled to the same or greater protection than that afforded to other internal deliberative information? For how long should such material be protected?

Question 3: What protection should there be for information which involves candid assessment of risks? For how long does such information remain sensitive?

Question 4: Should the executive have a veto (subject to judicial review) over the release of information? If so, how should this operate and what safeguards are required? If not, what implications does this have for the rest of the Act, and how could government protect sensitive information from disclosure instead?

Question 5: What is the appropriate enforcement and appeal system for freedom of information requests?

Question 6: Is the burden imposed on public authorities under the Act justified by the public interest in the public's right to know? Or are controls needed to reduce the burden of FoI on public authorities? If

controls are justified, should these be targeted at the kinds of requests which impose a disproportionate burden on public authorities? Which kinds of requests do impose a disproportionate burden?

The Commissioner set out his outline response in a lecture he gave to the LSE on 1 October – the ICO response will not seek to campaign and will seek to draw on the facts and experience from 10 years of overseeing compliance with the Act.

The Commission's review is expected to report before the end of the year.

2.3 Good Practice

Work includes:

We have a programme of workshops with Local Medical Committees (LMC) specifically targeted at providing GPs and their Practice Managers with practical advice. The first three have been well received.

The Communications Audit Team has completed risk analyses of the CSPs that are subject to Data Retention Notices and have developed a process for conducting site visits of CSPs. The team continues to liaise with the Home Office over a programme of visits and have established links with IOCCO to discuss issues relating to data retention.

We received 31 Snap Survey feedback responses to our self-assessment toolkit pilot. The results were overwhelmingly positive with 94% of users saying they would use the toolkit again. Suggestions for improvements were largely in keeping with existing plans and so work has begun to create a final version to be released online during Q3. The pilot feedback also provided a number of promotional contacts which we intend to utilise when the toolkit goes live.

Future Action:

We are attending the Solicitors' Regulatory Authority conference to promote awareness of Advisory Visits and to educate the sector more widely.

Under our European obligations we will be auditing the national SISII system at the Sirene Bureau at NCA and undertaking an additional visit to the Home Office Live Police Systems.

We are further developing our knowledge of the Integrated Care Pioneer Projects. The Health and Local Government audit teams are jointly planning visits to selected pioneer projects and NHS organisations/Local Authorities involved in these in order to understand and assess

approaches to the sharing of personal data required for the delivery of integrated care services. We hope to report on our findings towards the end of the year.

Outcomes:

We published outcome reports for dental practices (and the British Dental Association and the Medical Defence Union) and residential care homes (adult and child).

3. Government and Society Sector

3.1 Road signs for use of cameras

In 2014, after discussions and correspondence with the Department for Transport (DfT), they agreed to include a new prescribed sign for enforcement cameras in the draft road traffic sign regulations. This new sign would permit the name and crest of a local authority to appear on the enforcement camera traffic sign. These regulations were due to be introduced in March 2015 but this has not yet happened. We wrote to the DfT in April 2015 to express our concern over the delay in the introduction of the regulations.

Outcome:

After further correspondence and discussion with the DfT, they informed us that the regulations are now due to be introduced in March/April 2016. Nevertheless, DfT have said, until the regulations are introduced, if a local authority approaches them to ask for authorisation of a camera sign design including the authority's name as shown in the draft regulations, that despite the current moratorium on new prescribed road signs, the DfT will support the authority's request and write to the minister to break the moratorium.

DfT have agreed that we can publicise this exception to the moratorium and we are awaiting agreement from them to our suggested wording.

DfT have also recently issued a further consultation on the draft regulations, part of which asks for ideas and initiatives to reduce sign clutter. We have responded to this consultation to give our view that, in the long-term, it would be beneficial to set up a national government website identifying camera operators around the road network as part of GOV.UK that would provide the public with information about enforcement cameras.

Future work:

As part of ongoing work on a 'high profile case' involving a London local authority's use of traffic cameras we will inform them that they can now apply for authorisation of a camera enforcement sign with their name and that we expect them to make such an application so that they comply with the data protection principles. We will also publicise the exception to the moratorium among other local authorities.

We will advise local authorities that, as well as using new camera enforcement signs that include their names, they must now update their websites so that when individuals search on an authority's website they

can easily find out more information about that authority's use of cameras.

Contact: Jonathan Bamford, Sara Rolin

3.2 Government Departments: misleading websites

[Redacted]

3.3 Charities

Over the summer of 2015 a number of stories appeared in the media relating to the compliance of the charity fundraising sector with the requirements of the Data Protection Act and PECR.

A review of charity fundraising was launched by Rob Wilson, Minister for Civil Society and this review was carried out under the auspices of Sir Stuart Etherington of the National Council for Voluntary Organisations (NCVO). The Government has accepted the findings and recommendations of this review and has stated that it is supportive of a new Fundraising Regulator being set up to provide robust self-regulation in the charity fundraising sector.

Additionally the Public Administration and Constitutional Affairs Select Committee (PACAC) launched an Inquiry into fundraising in the charitable sector.

Outcome:

We worked with Policy Delivery and Enforcement colleagues to provide briefings to the Information Commissioner for his meeting with the Minister for Civil Society and his appearance before PACAC. The Commissioner also met with Sir Stuart Etherington as part of the review of fundraising self-regulation.

In addition we submitted written evidence from the ICO to the PACAC Inquiry emphasising the importance of the ICO Direct Marketing Guidance and the need for the charity sector to comply with the law as a minimum standard.

Future work:

We will continue to monitor Government actions and reaction from within the sector as new fundraising self-regulatory structures are set up. We will also seek to build a solid working relationship with the new Fundraising Regulator if and when it is set up.

We will update the strategic mapping of work with the charity sector to inform how we can engage effectively with the sector, not only on issues relating to PECR compliance, but also those relating to data sharing and security and with smaller charities as well as large fundraising organisations.

New examples specifically relating to charities are to be included in updated Direct Marketing Guidance and we will investigate which communications channels we can use to spread this guidance widely within the sector.

Contact: Judith Jones, Sara Rolin, Richard Marbrow

3.4 Independent Inquiry into Child Sexual Abuse (IICSA)

We were contacted by the Inquiry for advice in relation to the data protection issues arising from the Inquiry's letter to over 240 organisations requiring them to retain personal data. The ICO had already received enquiries on this issue.

Outcome:

Following a meeting with IICSA it was agreed that they would provide supplementary guidance for organisations which made clear that the continued preservation of data was necessary to address legal duties. The guidance would also include that this further clarification was issued following consultation with the ICO. We were also asked to provide the text for specific parts of the guidance. The guidance was published on the IICSA website in mid-August.

Customer Contact are now advising on the availability of the guidance and our input; also ICO Communications tweeted on the availability of the guidance.

Future work:

Formal lines of contact with IICSA have now been established, both in relation to their own compliance with relevant information rights legislation and also their remit.

Contact: Jonathan Bamford, Sue Markey

4. Police, Justice and Borders Sector

4.1 Police use of surveillance technologies

[Redacted]

4.2 High Profile case: British Transport Police

[Redacted]

4.3 Metropolitan Police Service (MPS) – Information Rights performance

[Redacted]

4.4 Investigatory Powers Legislation

[Redacted]

5. Public Services Sector

5.1 Secretary of State for Health's announcement of reviews for data security, the use of 'consent' models and the opportunity to object

The Care Quality Commission (CQC) have been asked to lead a review into data security in the organisations they regulate. The National Data Guardian (NDG) has also been asked to lead a review into 'consent' models and the opportunity to 'opt- out' of data sharing.

Across the health sector the security and the accuracy of the data held is known to be an issue. The developing uses of technology such as medical apps and the drive to achieve a paperless NHS is further enhancing the risks.

Within all organisations in the health and local government sectors there is a drive to use 'consent' models in order to share information. The recent announcement by the Secretary of State for Health that a review will be conducted into consent and objections has further increased awareness of the 'need' for consent.

The issue for information rights is the lack of understanding of the professionals and others in the differences between gaining consent for common law requirements and gaining consent under the DPA.

Outcome:

We continue to highlight to all our key stakeholders the importance of security, accuracy and fair processing and of recognising the differences between legislation and therefore when and the form in which consent is required or appropriate.

The Public Services team have accepted invitations by CQC and NDG to assist in the work of the reviews.

We have initiated conversations and jointly hosted a full day workshop with key influencers and decision makers within the sectors to ensure clarity and understanding of those who will implement procedures and that consistency is applied to the process.

Future work:

Working with the NDG, the Local Government Association and other influencing organisations we will continue to provide advice and support and to highlight the key issues. We will attend review meetings and provide input as and when required. On behalf of the NDG review of

consent we will be hosting a workshop to ensure review panel members understand the issues.

Contact: Dawn Monaghan

5.2 High Profile Case - Care.data disclosure objections

[Redacted]

5.3 The Integration of Health and Social Care

Integrated Care has become an overall banner for data sharing in the health and social care arena.

The data sharing can be health to health, health to local government and vice versa, local government to a group of multi-agencies including health, police and education organisations. Clearly whilst the principles remain the same, there are subtle differences in the issues encountered.

Outcome:

We have been identifying the different initiatives which are in the arena such as the pioneers programme, vanguard authorities, troubled families projects, care record projects etc. To date we have concentrated on building relationships with key players such as the Local Government Association (LGA) and the Centre of Excellence (CoE) and DH. We have then been identifying and capitalising upon opportunities to offer advice guidance and support.

As part of that work in conjunction with the new care models group we assisted in developing a decision tree for organisations when they are considering sharing data for integrated care.

Through our work on integrated care and consent models, it has become apparent that the way in which a data controller/data processor relationship is portrayed in DPA terms is not compatible with the way in which a system supplier is now engaged, nor does it reflect the responsibilities of the systems suppliers in the contemporary context. The impact of this could have detrimental and far reaching implications for both citizens and data controllers.

Future work:

It is predominately GPs as data controllers who are 'at risk' from the potential lack of compliance. Working with the British Medical Association we will ensure that GPs are fully aware of their responsibilities and how to remain compliant in this context. We will also be asking NHS England and

HSCIC what they intend to put in place in regard to information governance when engaging suppliers as systems of choice.

Contact: Andrew Rose

6. Business & Industry Sector

6.1 Safe Harbor

(The developments outlined below took place shortly after the period covered by this report. They are nevertheless included because of their significance).

On 6 October 2015 the CJEU issued its judgment in the case of Schrems v Irish Data Protection Commissioner. The judgment invalidated the 2000 decision of the European Commission declaring that the Safe Harbor, a self-regulatory system with statutory underpinning, provide adequate protection for personal data transferred from the EU to Safe Harbor member companies in the US. The judgment also made clear that despite the existence of a Commission decision on adequacy data protection authorities are not prevented from examining claims from individuals that their data are not properly protected when transferred.

The reasons why the CJEU invalidated the Commission decision were the ability of the US intelligence services to gain access to transferred personal data beyond that strictly necessary for their functions and the lack of any right for affected EU citizens to pursue legal remedies in the US.

The CJEU judgment has caused considerable concern amongst data controllers who rely on the Safe Harbor decision as the legal basis for their transfers of personal data to the US. We issued an immediate statement intended to calm fears and discourage data controllers from rushing to find alternative, and perhaps less satisfactory, legal bases for their transfers of personal data. These sentiments were echoed by us at an industry round table organised by the DCMS minister, Baroness Neville-Rolfe. We also took part in an extraordinary meeting of the Art 29 Working Party which issued a statement calling on member states and the EU institutions to open discussions with the US authorities to find political, legal and technical solutions. The ongoing negotiations on a new Safe Harbor could be part of the solution but if no solution has been found by the end of January 2016 EU data protection authorities are committed to take all necessary and appropriate actions.

Outcome:

ICO statement and participation in Ministerial round table have helped to calm immediate fears and prevent an inorderly rush to other, perhaps less privacy protective, transfer mechanisms. Contribution to Art 29 WP discussion has ensured that the WP's statement, whilst strongly worded, is nevertheless measured and proportionate.

Future Work:

Publication of further advice to businesses on the implications of the judgment and the options open to them. Participation in ongoing Art 29 WP activity analysing the wider impact of the judgment on transfer mechanisms other than the Safe Harbor.

Contact: David Smith

6.2 Electronic Identification and Trust Services (eIDAS) Regulations

[Redacted]

6.3 Open banking

[Redacted]

6.5 Insurers requiring subject access to medical records

[Redacted

6.6 Google privacy policy

[Redacted]

7. National Regions

7.1 Wales

7.1.1 NHS Wales: standards in information governance training

Following on from last quarter's reporting of the training audits of NHS Wales bodies, which had been undertaken as a consequence of the standard of IG training in NHS Wales appearing to be significantly lower than in other parts of the UK, this quarter saw us preparing and then disseminating the strategic level Summary Report to the Health Minister, NHS Wales' Chief Medical Officer, Health Board chief executives and Caldicott Guardians. The report included high level (national) recommendations, as opposed to the individual (Board-level) outcomes and requirements which had previously been forwarded to the participating Health Boards. The summary report was on the agenda at the Wales Information Governance Board (WIGB) meeting in July, and it also linked to a separate agenda item looking at the efficacy of C-PiP (the Welsh equivalent of England's IG Toolkit).

Outcomes: The Welsh Government has sent out a Circular to NHS Wales asking for input to a formal response to the ICO, which we await with interest. A meeting has also been set up for the next quarter with senior officials at the WG, including the Chief Medical Officer.

Future work: As a result of the summary report being presented at WIGB, at the Board's request we have undertaken to revisit the work in 2 years' time to review progress.

Contact: Anne Jones, Helen Phillips

7.1.2 Information Sharing

The issue of information sharing remains high on the agenda in Wales, with further meetings this quarter to update on the current position regarding the SPI programme and WASPI team (which are both due to end on 31 March next year), and featuring in the WG's Green Paper "Our Health, Our Health Service". We responded to the Green Paper, emphasising the importance of staff training and supporting continued funding for WASPI as an effective good practice tool. We also met with the Welsh Government's Local Partnerships team and the Wales Audit Office (WAO) to start planning for a short series of workshops on the importance of sharing information effectively in the new landscape of partnership working, and how to carry it out successfully and safely. The events will form part of the WAO's "Share the Learning" series of practical workshops, and will be introduced by Huw Vaughan Thomas, the Auditor General for Wales.

Future work: Further planning with the WAO and other key partners this quarter for January's "Dare to Share" workshops.

Contact: Anne Jones, Dave Teague

7.1.3 Local government liaison

The Welsh Government are shortly to announce plans to drastically reduce the number of local authorities in Wales. This is planned to happen by around 2020, and will present a number of information governance issues. To ensure the ICO is well-positioned to work with local authorities when these changes are introduced, we have started a liaison programme to build up good working relationships with appropriate staff in each authority. This quarter we have contacted several and offered a half-day open agenda meeting to discuss subjects of their choosing, or to meet with personnel that their IG contact feels will benefit most from a discussion with the ICO (eg IAOs).

Outcomes: We are already seeing improved working relationships in that a number of councils who are not known for getting in touch with us have done so for advice.

Future work: Continue with the programme of liaison work.

Contact: Dave Teague

7.2 Northern Ireland

7.2.1 Information rights good practice and compliance in NI legislative reform and development (Central Government)

Work includes:

Although facing an uncertain political future, the NI Government is continuing to progress legislative reform for citizens. During this period we have made a number of contributions to its proposals, including responses to consultations on the NI Mental Capacity Bill, the Housing (Amendment) Bill, the Justice No.2 Bill and the Health and Social Care (Control of Data Processing) Bill. As a consequence, the ICO is at the heart of the legislative process competently providing advice and clarification on the information rights aspects of reform as well as advising Government on the legislative requirements relevant to the changing landscape (including giving oral evidence on the Health and Social Care (Control of Data Processing) Bill.

Future work:

We also have been asked to provide oral evidence on the NI Mental Capacity Bill and the NI Housing (Amendment) Bill and are confident there will be further follow up with us on a number of the issues we have highlighted.

Outcome:

During a time of innovative legislative change as well as an uncertain political structure, the ICO have developed effective, informed and successful stakeholder relationships. This has ensured we are able to influence information rights practice at the highest legislative level as well as within policy and practice. Having been invited to give oral evidence to NI Assembly Committees on three occasions during this period, we are confident that there are clear tangible impacts from our engagement.

Contact: Shauna Dunlop, Ken Macdonald

7.2.2 Information rights good practice and compliance at the heart of NI legislative reform and development (Northern Ireland Civil Service)

Work includes:

Complementing the work with the NI Central Government, we have provided a formal response to a number of initiatives being taken forward by the NI Civil Service, such as a Strategy on Co-operating to Safeguard Child and Young People in NI and the draft NI Human Trafficking and Exploitation Strategy 2015-2016. We have also provided advice on aspects of the NI Justice Bill, including guidance for the Criminal Records Filtering Review Mechanism and draft Statutory Guidance for Chief Officers of Police.

Future work:

We will continue to engage with the NI Civil Service and related bodies to further influence and provide information rights compliance advice in the coming months.

Outcome:

Ensuing information rights practice and compliance is included at the policy design stage of government reform and practice. Maintaining effective and successful stakeholder relationships.

Contact: Shauna Dunlop, Rachael Gallagher

7.2.3 Health and Social Care (Control of Data Processing) Bill

Work includes:

In June 2015, and following an earlier consultation from the Department of Health, Social Services and Public Safety in October 2014 on a proposal to introduce legislation to allow for the secondary use of identifiable health and social care data in controlled circumstances to which we responded, the NI Minister for Health introduced the Health and Social Care (Control of Data Processing) Bill to the NI Assembly. The Committee for Health then sought our written opinion on the provisions of the draft Bill and we were subsequently invited to give oral evidence to the Committee in September.

Future work:

To continue to engage with the NI Assembly and the DHSSPS to provide advice further information as required.

Outcome:

In our written and oral evidence, we highlighted areas in which the Bill could be strengthened and we anticipate that amendments to it will follow.

Contact: Ken Macdonald, Rachael Gallagher

7.2.4 Southern Health and Social Care Trust – The management of sexual offender information in hospital settings

Work includes:

The Southern Health and Social Care Trust approached the ICO to review the draft protocol on sharing information relating to high risk sexual offenders where they presented at hospital either through pre-arranged appointments or for emergency care. The intention of the Protocol was to provide a procedure for Trust staff to follow, to ensure that they were sharing information in a proportionate and secure way in order to protect both members of the public and the offender. We provided good practice advice to ensure the protocol was data protection compliant and, in particular, recommended that the Trust carry out a Privacy Impact Assessment to identify any potential privacy impact upon individuals.

Future work: No future work is currently planned.

Outcome:

The Trust returned with an updated protocol having conducted a comprehensive PIA and having incorporated the outcomes into the revised document. In addition, the Trust gained tremendous value and learning from consulting with interested parties incorporating their views into the Protocol. The Protocol has now been agreed with the Police Service of Northern Ireland and the Public Protection Arrangements Northern Ireland, with a view to rolling this out across all five Health and Social Care Trusts areas in Northern Ireland.

Contact: Rachael Gallagher

7.2.5 Welfare Reform and NI Government Department Reform

Work includes:

As a part of the Stormont House Agreement of December 2014, it was agreed to implement a number of changes to the NI Welfare System. In anticipation of these changes, the responsible department, the Dept for Social Development (DSD), have held discussions with us regarding issues arising from the reform. As a consequence, we developed and delivered a one day training and awareness session on the practical use of PIA's to middle and senior managers within DSD.

Future work:

To continue to work with DSD as the proposals are developed.

Outcome:

Embedding a privacy by design approach to the development of new welfare payment systems.

Contact: Shauna Dunlop, Rachael Gallagher

7.2.6 Law Society of Northern Ireland – Data protection masterclass series

Work includes:

Following the success of our engagement with the legal profession in 2014/2015, we have built on this by providing a series of bespoke DP workshops to solicitors across Northern Ireland.

Future work:

We have also been invited to speak at Law Society of NI's Risk Management Conference which will be taking place in various locations across Northern Ireland in October.

Outcome:

Enhanced awareness in the legal sector regarding information rights and the work of the ICO.

Future work:

To keep in contact with the Law Society and the wider legal sector as required.

Contact: Rachael Gallagher, Shauna Dunlop

7.2.7 Local Government Reform in Practice

Work includes:

As part of an extensive programme of work with the local authority sector arising from the transition from 26 to 11 councils and the transfer of some planning powers to these authorities, and in partnership with the Department of the Environment and the Public Records Office NI (PRONI), we held a seminar on the application of the Environmental Information Regulations and other information rights legislation to the planning process.

Future work:

This was the final event in a year-long programme of seminars and workshops which we undertook in relation to the reform of local government in NI. Future work will be focused on the needs of individual councils whilst also working closely with the NI Local Government Staff Commission.

Outcome:

The engagement we have had with the councils has increased in queries from them, demonstrating their confidence in the ICO advice and policy and practice guidance and helping to improve compliance with the relevant legislation.

Contact: Shauna Dunlop

7.2.8 Voluntary and community sector engagement – NI Human Trafficking Charity

Work includes:

Following contact from a new Northern Ireland charity, Invisible Traffick, earlier this year, we developed and delivered a data protection awareness day to all volunteers of the charity, ahead of a plan to launch a dedicated helpline for individuals affected by human trafficking. The programme was tailored to the needs of the organisation - in particular, to ensure that the volunteers had an awareness of the data protection considerations of their work - and included a number of specific case-studies.

Future work:

As the helpline is due to begin in 2016, we have offered further assistance to the charity if they require and further information.

Outcome:

The charity now has understanding of the data protection issues relevant to their work, including practical considerations of exemptions and data sharing requirements. This understanding and commitment to a privacy by design approach from the outset will have significant benefits both to the data controller and individuals who will seek the help of the service. In addition this engagement complements our work in providing a formal written response to the draft NI Human Trafficking and Exploitation Strategy 2015-2016.

Contact: Shauna Dunlop, Rachael Gallagher

7.3 Scotland

7.3.1 Health & Social Care Integration

Work includes:

Providing advice and guidance to NHS Scotland and Scottish local authorities in relation to the Public Bodies (Joint Working) (Scotland) Act 2014, which requires that the provision of adult health and social care be integrated. The majority of Health Board areas have chosen to adopt the model which requires the establishment of an Integration Joint Board. This has implications for data controllership and much of the discussion has been around this issues. The work has also involved speaking to national conferences on the matter and widening the scope to include compliance in general with the DPA.

Future action:

Continued assistance and guidance to those institutions involved in the integration agenda. Continued speaking engagements to wider audiences to disseminate the DPA obligations on the existing and new institutions.

Outcomes:

Increased awareness and credibility of the ICO as regulator and source of authoritative advice and support.

Contact: Maureen Falconer

7.3.2 Recording of Named Person Data within Local Authority Education Systems via SEEMIS

Work includes:

Providing advice and guidance to a small working group established to take a project forward, driven by SEEMIS (an information management system for education) which seeks to establish a safe and secure storage and transmission facility for data in relation to the Named Person Service obligations under the Children & Young People (Scotland) Act 2014. This is a complex and complicated project not least because it is being driven by an organisation which currently provides the information management system for local authority schools in Scotland as a data processor. However, SEEMIS is owned by a majority of local authorities under a DC in Common arrangement. The complexity of the project is in the need for external agencies such as Police Scotland and the NHS to be able to share information in relation to children's wellbeing. The project is currently undergoing a Gateway Review to determine its status and viability. The ICO has been instrumental in questioning the proposals and providing some perspective.

Future action:

Participation in the Gateway Review and continued advice and guidance.

Outcomes:

Increased awareness of data protection among small third sector support organisations. Increased awareness and credibility of the ICO as regulator and source of authoritative advice and support.

Contact: Maureen Falconer

7.3.3 ICO Scotland Office Area Seminar Series in the Northern Isles

Work includes:

Provision of events on general data protection awareness and data sharing for local authorities, NHS Boards, voluntary sector and the Shetland Law Faculty in the Orkney and Shetland islands, including two half day conferences with circa 80 and 130 attendees respectively. In total, some 400 individuals attended 17 separate events in various locations between the two island group over 3.5 working days.

Future action:

We aim to hold similar events in other remote parts of Scotland on an annual basis.

Outcomes:

Increased awareness of data protection among multi-sector organisations. Increased awareness and credibility of the ICO as regulator and source of authoritative advice and support.

Contact: Ken Macdonald, David Freeland & Maureen Falconer

7.3.4 Human Trafficking and Exploitation (Scotland) Bill

Work includes:

The Human Trafficking and Exploitation (Scotland) Bill was introduced by the Scottish Govt in December 2014 and was passed by the Parliament on 1 October 2015. We provided written evidence to the Scottish Parliament's Justice Committee on the Bill and we subsequently met with Scottish Government officials to discuss our comments in detail and expand upon some the points made.

Future actions:

We will work with Scottish Government officials on regulations made under the Act which may specify personal information that has to be passed to the police in order to disrupt trafficking operations.

Contact: Ken Macdonald and David Freeland

7.3.5 Review of consensual stop and search

Work includes:

We spoke to John Scott QC, a leading human rights advocate who was appointed by the Scottish Government to chair an independent advisory group on Police Scotland's use of consensual stop and search. We identified a number of data protection issues that needed to be addressed including fair processing, whether children who are being stopped can reasonably give consent, and the collection and retention of telephone numbers.

The advisory group's report was published on 30 August and recommended that consensual stop and search should end. It also contains a draft Code of Practice for statutory stop and search which we will comment on in due course.

Outcomes:

Clarity of the legal basis upon which searches are being undertaken. Ensuring information obtained is necessary for, and limited to, the purpose.

Contact: Ken Macdonald and David Freeland

7.3.6 Law Society of Scotland

Work includes:

We have begun to work with the Law Society to identify opportunities to talk to smaller legal firms and sole practitioners about data protection. We have already spoken to the local law faculties in Glasgow and Shetland. We also have a date in the diary for the faculty in Edinburgh in early 2016. A recent undertaking with a law firm based in Scotland will also form part of our talk in future.

Future action:

With the Law Society, we will continue to identify further opportunities to talk to local faculties, particularly where we have other activities planned outside the Central Belt.

Outcomes:

Increased awareness and understanding of data protection in the legal sector. Better information security around client data. Continuing

engagement with the Law Society of Scotland to ensure professional guidelines build in the data protection principles.

Contact: David Freeland

8. International

8.1 Work with the Home Office on UK borders matters and processing of passenger data

As the 2015 Counter Terrorism Bill and Authority to Carry schemes have continued to become embedded, our liaison with the Home Office regarding the processing of Advance Passenger Information (API), Passenger Name Record (PNR) and exit check data has progressed and we continue to monitor for compliance complaints. [redacted]

Following the recent information gathering visit to the National Border Targeting Centre, work will continue to ensure the application of appropriate date protection safeguards.

The EU PNR Directive has progressed to the Trilogue stage, with some Member States strongly lobbying for the collection of intra-EU PNR. We were encouraged to see that a number of MEPs had taken on board the recommendations for greater data protection and privacy safeguards which had been made in the Article 29 opinion.

Next steps: In light of the above, the ICO will consider undertaking work with the carriers who collect API and PNR data for their own business purposes, with specific focus on the fair processing and accuracy principles.

The European Commission has opened formal negotiations with the Mexican authorities regarding the transfer of PNR data, although these talks will not be concluded until the Court of Justice of the European Union has ruled on the legality of the EU-Canada PNR agreement. This ruling could come before the end of 2015 and has potentially significant implications for travellers' data protection rights.

Contact: Hannah McCausland/Naomi Osborne-Wood

8.2 Europol/Eurojust/Customs/Eurodac/Schengen SIS II – large IT databases and information exchange at EU level for law enforcement purposes

Europol: We have taken steps to further establish our liaison with the Europol National Unit which is run out of the National Crime Agency. Next steps: Application of the data protection safeguards in relation to Europol's agreements with private parties and ICO responsibilities under the Europol Council decision will be discussed.
SIS II: The assessment by the European Commission and the Latvian Presidency of the UK implementation of the Schengen Information System II (SIS II) has been completed successfully.

The SIS II Guide of Access, detailing how data subjects can enforce their individual rights, has been updated to include the UK.
Next steps: An ICO post go-live audit will be carried out in the autumn.

Eurodac: On 20 July 2015 the Eurodac Recast system became operational in compliance with EU Regulation 603/2013. The new Eurodac system allows law enforcement agency, including the European Police Office (Europol), access to its fingerprints database, under strictly limited circumstances in order to prevent, detect or investigate serious criminal offences, including terrorism (Articles 5 and 7 of the Eurodac Recast Regulation).
Next steps: The ICO will keep in contact with the Home Office and the UK Visas and Immigration directorate.

Customs: Following a request by the European Data Protection Supervisor, the ICO established that the updated Customs Information System (CIS) security policy has been fully implemented by HMRC. Additionally we have confirmed that the guide to data protection responsibilities under the CIS Council Decision and the 2008 Data Protection Framework Decisions has been distributed and is being adhered to.
Next steps: The ICO will continue to liaise with HMRC regarding the limited amounts of personal data processed in the CIS.

Contact: Naomi Osborne-Wood

8.3 Article 29 (WP29) Working Party developments

Background and outcome:

Significant issues with implications for information rights (where these have not been referred to in other dedicated sections above) include:

- Working Party reaction (via press release) on the Decision of the Court of Justice of the European Union invalidating the EU Commission Safe Harbor Decision (see separate report on Safe Harbor);
- Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing;
- The Financial Matters subgroup is closely following the developments in the automatic exchange of tax information agreements and will be providing guidance on how these agreements should comply with data protection and privacy legislation.

Contact: Hannah McCausland/Naomi Osborne-Wood

8.4 International Enforcement Coordination and GPEN Committee

The ICO is a member of the Global Privacy Enforcement Network (GPEN) Executive Committee. The Committee has made further headway with a number of key projects for 2015 which should hopefully improve the way in which privacy enforcement authorities interact around the globe.

One of these projects is the 'Network of Networks'. The ICO led in signing up pilot participants to the Network of Networks projects, including with the International Conference of Data Protection and Privacy Commissioners, Common Thread Network and London Action Plan. This will pave the way for more regular communication and hopefully synergies in developing expertise between privacy enforcement networks around the world, which in the past risked becoming silos. A dedicated networks space has been created on the GPEN platform.

Next steps: The GPEN Side meeting will be held in Amsterdam at the International Conference on 27 October. The conference will also host the signing ceremony for the first eight authorities signing up the GPEN Alert Tool which allows sharing information in a secure and confidential way between authorities potentially interested in investigating/being involved in contacts on a case with cross-border implications.

Applications are now possible via the International Conference of Data Protection and Privacy Commissioners (ICDPPC) Secretariat for Authorities wishing to participate in the Global Cross Border Enforcement Cooperation Arrangement. The ICO intends to participate and will make the relevant application.

Contact: Hannah McCausland/Adam Stevens

8.5 Commonwealth 'Common Thread' Network of Data Protection Authorities

The ICO is a co-chair of this Network with the Office of the Privacy Commissioner of Canada (OPC).

The Network has continued developing its membership base.

In terms of practical activity, the Network has been working on its contribution to the Communique to be adopted at the Commonwealth Heads of Government Meeting (CHOGM) in Valletta in late 2015.

The Common Thread Network held a global member teleconference in August for all members.

Outcome:

Member engagement has increased.

The wording for CHOGM Declaration has been sent to the Maltese Ministry for consideration by all member delegations.

Future work:

The Network will also hold a side meeting at the International Conference of Data Protection and Privacy Commissioners in Amsterdam in October.

Malta is hosting the CHOGM Conference this year and the Maltese DPA has made (in liaison with the ICO and Canada's OPC as Co-chairs of the Common Thread Network) new proposals for the CHOGM Communique text on behalf of Common Thread to the Maltese ministry which is organising the CHOGM conference. The event will take place at the end of November.

Contact: Hannah McCausland

8.6 Spring Conference follow-up

The 27th Case Handling Workshop took place in Tirana, Albania, on 28 and 29 September 2015. The ICO nominated two representatives who presented on the case handling process and a year on from the *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* CJEU ruling (C-131/12), how search engine removal requests are handled.

Contact: Naomi Osborne-Wood

9. Enforcement

9.1 Anti-Spam Investigation Team; Criminal Investigation Team and Intelligence Hub

We issued a civil monetary penalty of £200,000 against Home Energy and Lifestyle Management Ltd for making circa 6 million automated calls in breach of the Privacy and Electronic Communication Regulations (PECR). This was the largest penalty issued by the ICO for nuisance calls.

This action followed two other civil monetary penalties for £50,000 against Point One Marketing Ltd, and £75,000 against Cold Call Elimination Ltd for making live unsolicited marketing calls to consumers.

We monitored six organisations this quarter which we believe represent risks in relation to adherence to PECR. We held two compliance meetings with organisations in order to improve direct marketing practices, and a further 13 meetings with charities, following concerns raised in July about their fundraising practices. The meetings with the charities will inform the ICO's ongoing investigation into whether those charities complied with the Data Protection Act and the PECR.

On 31 August, the First Tier Tribunal provided a decision following an appeal about an Enforcement Notice issued by the ICO against Optical Express Ltd for sending unsolicited marketing text messages. The Tribunal upheld the ICO's enforcement action. Optical Express have applied for permission to appeal the judgment.

We prosecuted Consumer Claims Solutions Limited for a non-notification offence. They pleaded guilty and received a fine of £200, with £393 in costs and a victim surcharge of £20. We also prosecuted Nuisance Call Blocker Limited for filing to respond to an Information Notice. The company failed to attend court and were found guilty in their absence. They were fined £2,500 with £493.85 costs and a victim surcharge of £120.

Three further prosecutions for non-notification offences are scheduled to take place in the next quarter. A trial for a section 55 offence is scheduled to take place in January 2016.

Operation Spruce remains the main criminal investigation activity and priority within the ICO. Officers from the ICO and National Crime Agency are still conducting interviews with witnesses throughout the UK.

We have continued to work on the International Enforcement Handbook in partnership with the Canadian OPC. The handbook will serve as a useful guide for DPA practitioners across the globe and will be presented at the

International Conference in October. Work is ongoing to support Case Officers within Enforcement when working on potential international issues.

Results of the GPEN Sweep 2015 (involving 29 countries), focusing on children's privacy, were released on 2 September and achieved international media coverage. A follow-up report has been produced and will inform our compliance activities through contact with the data controllers identified in the project.

Work has begun on the 2016 GPEN Sweep, which will be led by the ICO. This is a significant challenge and responsibility for the ICO.

The London Action Plan (LAP) held its annual conference in Dublin this July, when 14 countries and more than 40 members of the group attended. The LAP is an international meeting of regulators, agencies and organisations committed to tackling nuisance calls, and the ICO is part of the Secretariat along with Canada's CRTC and the US Federal Trade Commission.

At the conference, the LAP members agreed to work on a revised Memorandum of Understanding with the aim of working together more effectively, and sharing knowledge, skills and ideas for combatting unsolicited communications.

The ICO attended the first Insurance Fraud Disruption Committee (IFDC) meeting hosted by the Insurance Fraud Bureau. This will be a regular meeting to facilitate intelligence sharing between relevant regulators and law enforcement to support our work around data theft and unsolicited marketing used to enable insurance fraud. We also presented to the Insurance Fraud Enforcement Department to provide a better understanding of our regulatory powers and responsibilities.

Next Quarter

We will further progress the interview phase of Operation Spruce, the main criminal investigation priority of the ICO.

We will continue to prioritise our investigations and activities to maintain focus on effective enforcement of the PECR, and progression of concerns received since the change of law on 6 April 2015.

We will report on our investigation of charities and whether they contravened the Data Protection Act and the PECR.

We will report on a 'mystery shopping' exercise the ICO has been conducting since April, with the aim of better understanding the journey

of some unsolicited marketing and how individuals can better protect their personal data .

We will publish the first in a series of 'Data Cycles', which will aim to highlight and raise awareness about how people's personal information is being used.

We will chair the first GPEN Sweep 2016 international working group call and seek to decide a potential relevant topic area. A cross-office steering group will be created to support this work.

9.2 Civil Investigation Team

The intake of new cases created in Q2 was 474 with 392 cases closed.

96% of the cases assessed in Q2 were derived from self-reported breaches. This is an increase of 11% on the previous quarter.

317 cases are under active investigation at present. A further 168 cases have been triaged and remain with the team ahead of allocation for a substantive investigation.

Sector trends

The most significant work stream for DPA breaches continues to be the health sector. In the first quarter of this financial year health cases accounted for 49% of the cases risk assessed and this figure has remained consistent during the second quarter. We had identified a possible cause of increased breach reports from the health sector during the first quarter (a change in the IG toolkit led to some historical cases and cyber incidents (which are not IG incidents) being reported to ICO). However as this problem was resolved it does not account for the continued high receipts in the second quarter.

In common with our experiences in 2014/2015 and in the first quarter, Local Government also continues to dominate. In Q2 just under 11% of cases related to the local government sector, which again is consistent with the previous quarter's intake.

Monetary Penalties and formal regulatory action cases

We have issued one Civil Monetary Penalty this quarter, set at £180,000 following a serious contravention of principle seven of the Data Protection Act. The notice was issued to Money Shop following the theft of two servers, in two separate incidents. The servers contained customers' financial details.

We also issued two Notices of Intent during the second quarter. The first concerned an unsecured FTP server which led to thousands of client files being exposed. The case was not pursued beyond the Notice of Intent stage, following receipt of representations from the data controller. The second was issued following the theft of unencrypted DVD's containing witness testimony from the data processor.

At the time of writing, one additional recommendation to serve a penalty has been made and several other cases are at varying stages of the CMP process.

We are also in the process of preparing reports recommending that Enforcement Notices be issued to several organisations. An Enforcement Notice to be served on a local authority is in the final stages, following its failure to implement recommendations made by the ICO during Good Practice audits. The team is making fresh enquiries in the case of the practices of a haulage company. The company had placed equipment into drivers' cabs which recorded audio continuously when the engine was switched on. We were informed that the audio function had been switched off, however we have since been contacted again by drivers to explain this is not the case. A report that recommended serving an Enforcement Notice had previously been prepared, and the team will look to take enforcement action if the company has failed to switch off the audio recording as it had previously promised.

We have issued 11 undertakings across 14 individual cases. One undertaking of interest was issued to Cambridgeshire Community Services NHS Trust. The Trust had taken the decision to provide training every two years, despite the IG toolkit requiring training to be provided on an annual basis. The Trust reinstated annual training during the ICO's investigation; an undertaking was served to ensure the Trust achieves acceptable levels of training completion. Three further undertakings are presently in draft.

Other significant activity

At the start of 2015/16, a triage team was established with the aim of significantly reducing the number of unallocated cases in the civil investigation team queues. A pilot ran during the first quarter, and was reviewed in the second quarter. The team had been successful in reducing the unallocated queue by 50%. It will now continue on a more permanent basis, with additional resource. The aim of this work is to help us to prioritise our investigations more effectively.

We also began to allocate low-risk data loss cases to the remaining PID teams during Q2. This too should see a reduction in the number of cases handled by the civil team.

We continue to liaise with our DPA colleagues overseas in relation to Operation Pyrite, an investigation into alleged 'blacklisting'. Following significant delays in establishing the primacy of investigations overseas, jurisdiction is now close to being established.

Reports are being finalised in relation to Operation Linden (the initiative aimed at holding list brokers and lead generators to account) with a view to taking regulatory action in respect of the remaining organisations.

Operation Juniper is to be recommended for closure. This is because no substantive evidence of contemporary blacklisting has been uncovered.

Six Local Government workshops, aimed at improving compliance within Adult and Children Services Departments, have now taken place. A further two workshops are scheduled during Quarter 3 2015/2016. Feedback from the workshops remains positive and the events have been well attended. A revised version of the presentation was delivered as a webinar in July, to allow delegates that had not been able to attend in person, and those working outside the local government sector, to attend.

Operation Gabbro – the enforcement case which sat behind this initiative has been concluded. The remaining matters regarding HSCIC and their commitment to address the NHS Spine address accuracy issues are to be taken forward by Strategic Liaison.

We served an Enforcement Notice on Google Inc. ordering them to delist nine search results relating to a named complainant.

Next quarter

Two further local government workshops will take place: one in Bristol and a final event at Manchester Airport.

Members of the Civil and Good Practice teams are exhibiting at the SRA conference in October.

Data security incidents (breaches of the seventh data protection principle) are a major concern for data subjects and a key area of action for the ICO. In response to the risks identified from breaches brought to the ICO's attention, the first Data Loss Threat Assessment will be published in Quarter 3. Its aim is to raise awareness for organisations of the high risk sectors and breach types.

It will also identify opportunities for campaigns and initiatives and enable prioritisation of our resources and investigations to identify suitable opportunities for enforcement action.

We have developed a strategy aimed at improving the performance of data controllers in respect of non-compliance with Subject Access Requests. The aim of the strategy is to undertake targeted enforcement action in respect of those data controllers which fail to respond substantively, or at all, to a subject access request. We anticipate that the first cases to be considered under this strategy will dealt with in the next quarter.

10. Performance Improvement

Notwithstanding, we continue to deal with the complaints from the public and use them to prompt changes in organisational practice. We referred a number of non-response subject access cases for formal enforcement action. At least one case was significant because of the nature of the request. It relates to a request from a third party for a relative's personal information. The organisation is challenging the right for the individual to make the request and our interpretation of the DPA in the specific circumstances. We continue to work on agreeing undertakings with a particular council and are awaiting a response and have written to one London Borough in connection with numerous delayed subject access responses.

The PID Police & Justice sector continued its programme of liaison meetings with the Home Office, Ministry of Justice and Metropolitan Police Service. The MPS provided evidence of ongoing performance improvements. An action plan for improved data protection practice was obtained from the Humberside, Lincolnshire and North Yorkshire Community Rehabilitation Company Ltd.

Our Freedom on Information monitoring activity continues. We informed the Ministry of Justice that we will monitor their performance in relation to FOI requests received between 1 September 2015 and 30 November 2015. The Royal Borough of Greenwich Council, which was the subject of an extended period of monitoring was taken off formal monitoring during the quarter following sustained improvements in performance. Cumbria County Council, Nottingham City Council and Salford City Council were also taken off formal monitoring in this period after showing a turnaround in performance too. We also wrote to all of the Northern Ireland Departments regarding FOI performance and provision of FOI statistics going forward, this is in the light of proposed departmental restructuring from April 2016.

It has been a busy quarter in the general business sector. We attended the Scottish DP Financial Services Forum in September. This was just after the 'most complained about' data was released and gave organisations the opportunity to ask questions and gain a better understanding of our decision to share this information more widely. We met with British Gas in order to build a more effective working relationship with them. The meeting was highly productive and we have committed to providing quarterly updates on concerns raised against them in order to assist them with their ongoing compliance.

We have had the opportunity to improve practice in the insurance sector. One insurance company was retaining call recordings which included credit card details and the three-digit security CVV number. The

organisation confirmed that this information was retained for 14-months. ICO Policy advice was that retention of this information was excessive and our dialogue with the company achieved a positive outcome whereby call recording is now to be paused whilst card details are given. A concern was also raised about another insurance company where marketing material was being sent to customers who had opted out, via their renewal notices. When this was raised with the organisation, they initially said that they couldn’t make the necessary changes until their infrastructure was changed in the next 3–5 years. Following ICO policy advice we advised that prompt action was needed and gave advice on how they might make changes to become compliant. The organisation has now made the necessary changes.